In re Application of: Ariel PELED et al
Serial No.: 10/748,178
Filed: December 31, 2003
Office Action Mailing Date: May 11, 2010

Examiner: GYORFI Thomas A.
Group Art Unit: 2435
Attorney Docket: 27153
Confirmation No.: 5563

In the Claims:

1. (Currently Amended) A method for computer workstation based information protection, the method comprising:

a) monitoring a user's actions on said computer workstation;

b) detecting whether content in use at said workstation in association with said actions being monitored comprises confidential information, said detecting comprising performing a statistical analysis of said content in use by said user using identifiers from a content identifier database, said statistical analysis using said identifiers to associate said content with respective confidential information, said confidential information being associated with respective predefined policies;

c) analyzing said monitored action with respect to a respective pre-defined policy associated with any confidential information identified by said analysis as being associated with said content in use at said workstation, to determine whether said actions prejudice said confidential information; and

d) executing said policy in accordance with the results of said determination to control said actions; and wherein, in the event of two or more conflicting policies being found, a strictest one of the policies is identified and used.

2. (Original) A method according to claim 1, wherein said policy comprises restrictions on at least one of the following actions: print, save, copy, autosave, fax.

3. (Original) A method according to claim 1, wherein said monitoring said user's actions on said workstation comprises detection of indications of attempts at tampering.

4. (Original) A method according to claim 3, wherein said detection of indications of attempts at tampering comprises obtaining logical indications or statistical indications.

5. (Original) A method according to claim 3, wherein said detection of indications of attempts of tampering comprises detection of at least one un-certified add-in.

6. (Original) A method according to claim 5, wherein said detection includes noting that said un-certified add-in is hooked to events of a local operating system.

7. (Original) A method according to claim 3, wherein said detection of indications of attempts at tampering comprises detection of at least one debugging technique.

8. (Original) A method according to claim 7, wherein said debugging technique comprises use of any of: a debugger, a virtual machine, a software emulator, a software trap, and a remote administration tool.

9. (Original) A method according to claim 3, wherein said policy comprises restrictions of actions made available to said user upon said detection of indications of attempts of tampering.

10. (Original) A method according to claim 9, wherein said restrictions of user's actions upon said detection of indications of attempts of tampering comprise applying restrictions on actions within a software application operable to process said information.

11. (Original) A method according to claim 3, wherein said execution of said policy comprises performing at least one action upon detection of indications of attempts of tampering.

12. (Original) A method according to claim 11, wherein said actions comprise at least one of the following: encrypting at least one buffer, and encrypting at least one shared memory.

13. (Original) A method according to claim 11, wherein said actions comprise preventing the decryption of encrypted digital content.

14. (Original) A method according to claim 1, wherein said pre-defined policy is defined with respect to a software application on said user's workstation.

15. (Original) A method according to claim 1, wherein said policy comprises reporting about attempts to perform actions that do not comply with an organizational policy or about attempts to perform actions that are suspected to not comply with the organizational policy.

16. (Original) A method according to claim 1, wherein said policy comprises performing logging of attempts to perform actions that that do not comply or are suspected to not comply with the organizational policy.

17. (Original) A method according to claim 1, wherein said information protection comprises protecting information held within a software data processing application able to process said information.

18. (Original) A method according to claim 17, wherein said software data processing application operates in conjunction with a software client.

19. (Original) A method according to claim 17, wherein said software client is a tamper-resistant software client.

20. (Original) A method according to claim 17, wherein said software client is operable to monitor said user's actions and to execute said policy.

21. (Original) A method according to claim 17, wherein said software client is operable to detect information based on statistical identifiers residing in a specialized database.

22. (Original) A method according to claim 17, wherein said software client is further operable to detect events of said software application.

23. (Original) A method according to claim 22, wherein said events comprise events required for any of: printing said information; copying said information; storing said information, and displaying said information.

24. (Original) A method according to claim 1, wherein said policy further comprising managing usage rights.

25. (Original) A method according to claim 24, wherein said usage rights are determined according to any of: the classification of the document; the classification level of the user, and the authentication level of the user.

26. (Original) A method according to claim 24, wherein said usage rights comprise any of: viewing at least part of said information; modifying at least part of said information; sending at least part of said information to a recipient; storing at least part of said information; storing at least part of said information by an application; storing at least part of said information by a file system; storing at least part of said information in a portable device; storing at least part of said information in a removable media; storing at least part of said information portable storage device that is connected to said workstation using a USB port; pasting at least part of said information into a document; printing at least part of said information; printing at

least part of said information to file; printing at least part of said information to a fax, and printing a screen view document.

27. (Original) A method according to claim 24 wherein said policy further comprises definitions of actions to be performed.

28. (Original) A method according to claim 27, wherein said actions comprise any of: enabling usage of at least part of said information; disabling usage of at least part of said information; restricting the usage of at least part of said information, according to a pre-determined set of restrictions; reporting about the usage of at least part of said information, and monitoring the usage of at least part of said information.

29. (Original) A method according to claim 28, wherein said restriction of usage imposes requiring encryption of at least part of said protected information.

30. (Original) A method according to claim 29, wherein said required encryption is such that corresponding encrypted information can be decrypted only by a secure client.

31. (Original) A method according to claim 28, wherein said restriction of usage requires said protected information to reside on a secure server.

32. (Original) A method according to claim 31, comprising arranging a connection between said secure server and said workstation such that the transport between said secure server and said workstation is protected.

33. (Original) A method according to claim 32, wherein said protected transport comprises an encrypted transport.

34. (Original) A method according to claim 29, wherein said encryption of protected information further comprising encryption of a file comprising at least part of said protected information wherein said file is at least one of the following: temporary file and auto-recovery file.

35. (Original) A method according to claim 31, wherein said protected information further comprises a file comprising at least part of said protected information, wherein said file comprises any of temporary file and auto-recover file.

36. (Original) A method according to claim 17, wherein said software client authenticates itself to a server before at least some of the sessions.

37. (Original) A method according to claim 36, wherein said authentication depends on a classification level assigned to said protected information.

38. (Original) A method according to claim 36, wherein said authentication comprises any of: password based authentication; and network address based authentication.

39. (Original) A method according to claim 17, wherein said software client comprises components that can be automatically replaced.

40. (Original) A method according to claim 31, wherein said secure server employs cryptographic encryption of at least one file containing said protected information.

41. (Original) A method according to claim 31, wherein communication with said server is substantially transparent to said user.

42. (Original) A method according to claim 17, wherein in accordance with said policy said protected information is encrypted utilizing the encryption capabilities of said software application.

43. (Original) A method according to claim 42, wherein said software application operable to process said information is any of: a word processing application; Microsoft "word"; Open office "word", and Star office "word".

44. (Original) A method according to claim 17, wherein said software application comprises a control flag imparting a status of either read only or lock to a corresponding file, and wherein file modification within said software application which is operable to process said information is disabled via said flag.

45. (Original) A method according to claim 44, wherein said disabling of said file modification is controlled by said policy.

46. (Original) A method according to claim 1, wherein said policy comprises adding forensic information to said protected information.

47. (Original) A method according to claim 17, wherein said software client replaces the clipboard functionality of said software application thereby to process said protected information with a secure clipboard functionality.

48. (Original) A method according to claim 47, wherein said protected information copied into said secure clipboard is stored in an internal data structure inaccessible to other applications.

49. (Original) A method according to claim 17, wherein said software client is installed automatically from a remote server.

50. (Original) A method according to claim 49, wherein said installation of said software client utilizes anti-virus installation infrastructure.

51. (Original) A method according to claim 17, wherein updates of said software client utilize anti-virus update infrastructure.

52. (Original) A method according to claim 17, wherein at least part of the software code of said software client resides in an encrypted form.

53. (Original) A method according to claim 17, wherein at least part of the software code of said software client is attached to hardware of said computer workstation.

54. (Original) A method according to claim 17, wherein said software client is operable to automatically add information to said protected information in accordance with said policy.

55. (Original) A method according to claim 54, wherein said added information comprises any of: a document header; a document footer; and a textual disclaimer.

56. (Original) A method according to claim 17, wherein said client software is operable to open file that comprises said protected information only while connected to at least one server.

57. (Original) A method according to claim 56, wherein said servers enforce a policy with respect to said protected information.

58. (Original) A method according to claim 57, wherein said policy implies a set of restrictions regarding the usage of the said protected information.

59. (Original) A method according to claim 17, wherein said client software is operable to check that it is connected to a predetermined server before decrypting a file that comprise said protected information.

60. (Original) A method according to claim 59, wherein said servers enforce a policy with respect to said protected information, and wherein said policy comprises a set of restrictions regarding the usage of the said protected information.

61. (Original) A method according to claim 56, wherein at least two servers are operable to define said policy.

62. (Cancelled)

63. (Currently Amended) A method according to claim ~~62~~ 1, wherein in the event of two or more conflicting policies being found, a policy comprising the union of restrictions of said policies is used.

64. (Original) A method according to claim 56, wherein connection to at least two servers are required in order to determine said policy.

65. (Original) A method according to claim 56, wherein said server authenticates the integrity of said client by requiring a cryptographic hash of at least part of said client's software.

66. (Previously Presented) A method according to claim 65, wherein said cryptographic hash is with respect to a random address in said clients software.

In re Application of: Ariel PELED et al
Serial No.: 10/748,178
Filed: December 31, 2003
Office Action Mailing Date: May 11, 2010

Examiner: GYORFI Thomas A.
Group Art Unit: 2435
Attorney Docket: 27153
Confirmation No.: 5563

67. (Original) A method according to claim 56, wherein said client is entangled with said server's software, such that a functioning stand-alone copy of said client's software does not exist.

68. (Original) A method according to claim 56, wherein said method comprises at least two levels of protection, and wherein said levels of protection are operable to be configured as a function of the secrecy of said protected information.

69. (Original) A method according to claim 68, wherein in the most secure of said levels of protection, said protected information can only be accessed while connected to said server.

70. (Original) A method according to claim 68, wherein in at least one of said levels of protection, said information can be accessed for a limited time after the connection with said server was terminated.

71. (Original) A method according to claim 68, wherein in at least one of said levels of protection, said information can be accessed until the end of a current login session.

72. (Original) A method according to claim 68, wherein in at least one of said levels of protection, said information can be unlimitedly accessed after the server approves said information.

73. (Currently Amended) A method for information protection, said information comprising information items, said information being for usage on a computer workstation, comprising:

a) defining an information protection policy with respect to an information item, said defining comprising determining at least one measure, required to be enforced by said workstation, in said policy to protect said information item;

b) using identifiers obtained from a content identifier database performing a statistical analysis of content in use on said computer workstation to identify said information item as comprising confidential information to a given level of confidence, and

c) allowing said usage on a computer workstation of content comprising said information item only while said required measures in said policy are being applied by said workstation in view of said level of confidence; and wherein, in the event of two or more conflicting policies being related to said information item, a strictest one of the policies is identified and used.

74. (Original) A method according to claim 73, wherein said information protection measures comprises protecting information within a client software application.

75. (Original) A method according to claim 74, wherein said protecting information within a client software application comprises disabling at least one of the controls of said application.

76. (Original) A method according to claim 73, wherein said information protection measures comprises encryption of the memory of a graphic card or a video card.

77. (Original) A method according to claim 73, wherein said information protection measures comprises forcing a video card or a graphic card to a mode that causes no meaningful information to be stored in said video card's memory.

78. (Original) A method according to claim 73, wherein said information protection measures comprises scanning at least one storage device and identifying the existence of pre-defined information objects.

79. (Original) A method according to claim 78, wherein said pre-defined information objects comprise confidential information objects.

80. (Original) A method according to claim 73, wherein said information protection policy comprises at least one rule regarding at least one event of at least one software application operable to handle said information.

81 - 106. (Cancelled)

107. (Currently Amended) A method for computer workstation based information protection, the method comprising:

a) detecting an event occurring at said workstation, said event being associated with content;

b) performing a statistical analysis of said content associated with said event to identify confidential information within said content, said statistical analysis utilizing an identifier extracted from a content identifier database, said statistical analysis providing said identification; and

c) employing information protection based on an assessment of an importance of said event to protection of said confidential information, said assessment identifying at least one policy, and ; and wherein, in the event of two or more conflicting policies being found, a strictest one of the policies is identified and used.

108. (Original) A method according to claim 107, further comprising: handling an event, said event being designated as directing information protection, and employing a said information protection technique in reaction to said event.

109. (Original) A method according to claim 108, wherein said event comprise any of: loading a local operating system; loading an application; user action;

presenting a specific information into the system; an event generated by another system; suspicious activity; operating system time event; and a network time event.

110. (Currently Amended) A system for computer workstation based information protection, the system comprising:

i) a monitor configured for monitoring a user's actions on said computer workstation, said actions being associated with content;

ii) an analyzer associated with a content identifier database, said analyzer configured for:

performing a statistical analysis of said associated content in use by said user using content identifiers from said database to identify confidential information in said content, said identifying being provided with a level of confidence; and

analyzing said actions with respect to a pre-defined policy associated with said identified confidential information to determine whether said actions prejudice said information; and

iii) a policy execution module configured for executing said policy in accordance with the results of said analysis, including said level of confidence, to control said actions in accordance with said policy; and wherein, in the event of two or more conflicting policies being found, a strictest one of the policies is identified and executed.

111. (Original) A system according to claim 110, wherein said policy comprises restrictions on at least one of the following actions: print, save, copy, autosave, fax.

112. (Original) A system according to claim 110, wherein said monitoring said user's actions on said workstation comprises detection of indications of attempts at tampering.

In re Application of: Ariel PELED et al
Serial No.: 10/748,178
Filed: December 31, 2003
Office Action Mailing Date: May 11, 2010

Examiner: GYORFI Thomas A.
Group Art Unit: 2435
Attorney Docket: 27153
Confirmation No.: 5563

113. (Original) A system according to claim 112, wherein said detection of indications of attempts of tampering comprises detection of at least one un-certified add-in.

114. (Original) A system according to claim 113, wherein said detection of indications of attempts at tampering comprises detection of at least one debugging technique.

115. (Original) A system according to claim 112, wherein said policy comprises restrictions of actions made available to said user upon said detection of indications of attempts of tampering.

116. (Original) A system according to claim 115, wherein said restrictions of user's actions upon said detection of indications of attempts of tampering comprise applying restrictions on actions within a software application operable to process said information.

117. (Original) A system according to claim 116, wherein said software data processing application operates in conjunction with a tamper-resistant software client.

118. (Original) A system according to claim 117, wherein said software client is operable to monitor said user's actions and to execute said policy.

119. (Original) A system according to claim 117, wherein said software client is operable to detect information based on statistical identifiers residing in a specialized database.

120. (Original) A system according to claim 117, wherein said software client is further operable to detect events of said software application.

In re Application of: Ariel PELED et al
Serial No.: 10/748,178
Filed: December 31, 2003
Office Action Mailing Date: May 11, 2010

Examiner: GYORFI Thomas A.
Group Art Unit: 2435
Attorney Docket: 27153
Confirmation No.: 5563

121. (Original) A system according to claim 110, wherein said policy further comprising managing usage rights.

122. (Original) A system according to claim 121, wherein said usage rights comprise any of: viewing at least part of said information; modifying at least part of said information; sending at least part of said information to a recipient; storing at least part of said information; storing at least part of said information by an application; storing at least part of said information by a file system; storing at least part of said information in a portable device; storing at least part of said information in a removable media; storing at least part of said information portable storage device that is connected to said workstation using a USB port; pasting at least part of said information into a document; printing at least part of said information; printing at least part of said information to file; printing at least part of said information to a fax, and printing a screen view document.

123. (Original) A system according to claim 117, wherein said client software is operable to check that it is connected to a predetermined server before decrypting a file that comprise said protected information only while connected to at least one server.

124. (Original) A system according to claim 123, wherein said servers enforce a policy with respect to said protected information, and wherein said policy comprises a set of restrictions regarding the usage of the said protected information.

125. (Original) A system according to claim 116, wherein said software application operable to process said information is any of: a word processing application; Microsoft "word", Open office "word", and Star office "word".

126. (Original) A system according to claim 117, wherein said software client replaces the clipboard functionality of said software application thereby to process said protected information with a secure clipboard functionality.

127. (Original) A system according to claim 117, wherein said software client is installed or updated automatically from a remote server.

128. (Original) A system according to claim 127, wherein said installation or updates of said software client utilize anti-virus installation infrastructure.

129. (Original) A system according to claim 127, wherein said software client is operable to automatically add information to said protected information in accordance with said policy.

130. (Currently Amended) A system for information protection, said information comprising information items, said information being for usage on a computer workstation, the system comprising:

a) a policy reference monitor configured for identifying particular information items as requiring protection, defining respective information protection policies with respect to said identified information items, said defining comprising determining measures required to protect said information, said policy reference monitor further configured to place in a content identifier database an identifier for any such information for which a policy has been defined; and wherein, in the event of two or more conflicting policies being defined, a strictest one of the policies is identified and used;

b) a policy execution module configured for using said identifiers in a statistical analysis of content being used at said workstation to identify information items for which a policy has been defined, said identifying comprising providing a level of confidence, and for allowing said usage on a computer workstation of information comprising said items for which an information protection policy is

defined only while said required measures are being applied in view of said level of confidence.

131 – 146. (Cancelled)

147. (Previously Presented) A method according to claim 1, wherein controlling a user's action comprises at least one of: preventing said action, modifying said action, restricting, said action, monitoring said action, or logging said action.

148. (Previously Presented) A system according to claim 110, wherein to control an action comprises at least one of: preventing said action, modifying said action, restricting, said action, monitoring said action, or logging said action.

149. (New) A method for computer workstation based information protection, the method comprising:

a) monitoring a user's actions on said computer workstation;

b) detecting whether content in use at said workstation in association with said actions being monitored comprises confidential information, said detecting comprising performing a statistical analysis of said content in use by said user using identifiers from a content identifier database, said statistical analysis using said identifiers to associate said content with respective confidential information, said confidential information being associated with respective predefined policies;

c) analyzing said monitored action with respect to a respective pre-defined policy associated with any confidential information identified by said analysis as being associated with said content in use at said workstation, to determine whether said actions prejudice said confidential information; and

d) executing said policy in accordance with the results of said determination to control said actions; wherein in the event of two or more conflicting policies being found, a policy comprising the union of restrictions of said policies is used.

In re Application of: Ariel PELED et al
Serial No.: 10/748,178
Filed: December 31, 2003
Office Action Mailing Date: May 11, 2010

Examiner: GYORFI Thomas A.
Group Art Unit: 2435
Attorney Docket: 27153
Confirmation No.: 5563